

APPLICATION FOR UNITED STATES LETTERS PATENT

For

SYSTEM AND METHOD TO ACCESS SECURE INFORMATION RELATED
TO A USER

Inventor:

RONALD C. CARD

Prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026
(408) 947-8200

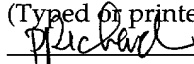
"Express Mail" mailing label number: EL351954353US

Date of Deposit: December 6, 2001

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Commissioner for Patents, Washington, D. C. 20231

Patricia M. Richard

(Typed or printed name of person mailing paper or fee)


(Signature of person mailing paper or fee)

December 6, 2001

(Date signed)

SYSTEM AND METHOD TO ACCESS SECURE INFORMATION RELATED TO A USER

RELATED APPLICATIONS

[0001] The present application claims the benefit of United States Provisional Patent Application Serial Number 60/254,456, filed on December 07, 2000, and entitled "USING A HAND-HELD ELECTRONIC DEVICE WITH BIOMETRIC CONTROL, SUCH AS A DIGITAL WALLET, AS A SECURE ACCESS POINT TO A SERVER, WEB SITE, OR MACHINE."

FIELD OF THE INVENTION

[0002] The present invention relates generally to electronic commerce transactions, and, more particularly, to a system and method to access secure information related to a user.

BACKGROUND OF THE INVENTION

[0003] Electronic commerce is achieving widespread use. Transactions are performed everyday over the Internet and through point of sale (POS) or bank systems. Such transactions are typically performed after the person requesting access to some information is authenticated and access is given to that person's private information, such as financial, medical, or other type of restricted records. Present systems are designed to maintain the integrity of the user's credit card, debit card, and account number. However, no measures are taken to ensure the secure authentication of the user in order to prevent unauthorized access by a potential thief.

[0004] Presently, applications providing access to sensitive information are based upon information that a potential thief may appropriate with relative ease. For example, some of the information presently required to grant access to sensitive material, such as a person's Social Security Number, date of birth, or mother maiden's name, is readily available. Once a potential thief collects any two pieces of this information, the thief may obtain access to the person's financial, medical, or other private information. In addition, most secure access systems are set up to divulge a person's entire file, once they receive the appropriate password and/or correct answers to the security questions. Therefore, a potential thief may steal the person's identity and ruin that person's credit.

SUMMARY OF THE INVENTION

[0005] A system and method to access secure information related to a user are described. Identification information related to a user is transmitted to an authentication entity. Access to a secure entity coupled to the authentication entity is received if authentication information identifying the user is provided to the secure entity.

[0006] Other features and advantages of the present invention will be apparent from the accompanying drawings and from the detailed description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The present invention is illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like references indicate similar elements and in which:

[0008] **Figure 1** is a simplified block diagram of one embodiment of a secure transaction system.

[0009] **Figure 2** is a simplified block diagram of one embodiment of a privacy card for a personal transaction device.

[0010] **Figure 3** is a simplified block diagram of one embodiment of a digital wallet for a personal transaction device.

[0011] **Figure 4** is a block diagram of one embodiment of a system to access secure information related to a user.

[0012] **Figure 5** is a flow diagram of one embodiment of a method to access secure information related to a user from the perspective of a personal transaction device.

[0013] **Figure 6** is a flow diagram of the method to access secure information related to a user from the perspective of an authentication entity.

[0014] **Figure 7** is a flow diagram of the method to access secure information related to a user from the perspective of a secure entity storing the information.

[0015] **Figure 8** is a block diagram of an exemplary digital processing or computing system in which the present invention can be implemented.

DETAILED DESCRIPTION

[0016] In the following descriptions for the purposes of explanation, numerous details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that these specific details are not required in order to practice the present invention. In

other instances, well-known electrical structures or circuits are shown in block diagram form in order not to obscure the present invention unnecessarily.

[0017] A system and method to access secure information related to a user are described in detail below. In one embodiment, identification information related to a user is transmitted to an authentication entity. Access to a secure entity coupled to the authentication entity is received if authentication information identifying the user is provided to the secure entity.

[0018] **Figure 1** is a simplified block diagram of one embodiment of a secure transaction system, which may be used in electronic commerce. As illustrated in **Figure 1**, in this embodiment, a transaction privacy clearing house (TPCH) 115 interfaces a user (consumer) 140 and a vendor 125. In this particular embodiment, a personal transaction device (PTD) 170, e.g., a privacy card 105, or a privacy card 105 coupled to a digital wallet 150, is used to maintain the privacy of the user while enabling the user to perform transactions. In an alternate embodiment, the PTD 170 may be any suitable device that allows unrestricted access to TPCH 115. The personal transaction device information is provided to the TPCH 115 that then indicates to the vendor 125 and the user 140 approval of the transaction to be performed.

[0019] In order to maintain confidentiality of the identity of the user 140, the transaction device information does not provide user identification information. Thus, the vendor 125 or other entities do not have user information but rather transaction device information. The TPCH 115 maintains a secure database of transaction device information and user information. In one embodiment, the

TPCH 115 interfaces to at least one financial processing system 120 to perform associated financial transactions, such as confirming sufficient funds to perform the transaction, and transfers to the vendor 125 the fees required to complete the transaction. In addition, the TPCH 115 may also provide information through a distribution system 130 that, in one embodiment, can provide a purchased product to the user 140, again without the vendor 125 knowing the identification of the user 140. In an alternate embodiment, the financial processing system 120 need not be a separate entity but may be incorporated with other functionality. For example, in one embodiment, the financial processing system 120 may be combined with the TPCH 115 functionality.

[0020] In one embodiment, the financial processing system (FP) 120 performs tasks of transferring funds between the user's account and the vendor's account for each transaction. In one embodiment, the presence of the TPCH 115 means that no details of the transactions, other than the amount of the transactions and other basic information, are known to the FP 120. The TPCH 115 issues transaction authorizations to the FP 120 function on an anonymous basis on behalf of the user over a highly secure channel. The FP 120 does not need to have many electronic channels receiving requests for fund transfer, as in a traditional financial processing system. In one embodiment, a highly secure channel is set up between the TPCH 115 and the FP 120; thus, the FP 120 is less vulnerable to spoofing.

[0021] In one embodiment, the TPCH 115 contacts the FP 120 and requests a generic credit approval of a particular account. Thus, the FP 120 receives a

minimal amount of information. In one embodiment, the transaction information, including the identification of goods being purchased with the credit need not be passed to the FP 120. The TPC 115 can request the credit using a dummy charge ID that can be listed in the monthly credit statement sent to the user, so that the user can reconcile his credit statement. Further, the personal transaction device 105 can include functionality to cause the credit statement to convert the dummy charge ID back to the transactional information so that the credit statement appears to be a conventional statement that lists the goods that were purchased and the associated amount charged.

[0022] A display input device 160 (shown in phantom) may be included to enable the user, or in some embodiments the vendor 125, to display status and provide input regarding the PTD 105 and the status of the transaction to be performed.

[0023] In yet another embodiment, an entry point 110 interfaces with the personal transaction device 170 and also communicates with the TPC 115. The entry point 110 may be an existing (referred to herein as a legacy POS terminal) or a newly configured point of sale (POS) terminal located in a retail environment. The user 140 uses the PTD 170 to interface to the POS terminal in a manner similar to how credit cards and debit cards interface with POS terminals. The entry point 110 may also be a public kiosk, a personal computer, or the like.

[0024] The system described herein also provides a distribution functionality 130 whereby products purchased via the system are distributed. In one embodiment, the distribution function 130 is integrated with the TPC 115 functionality. In

an alternate embodiment, the distribution function 130 may be handled by a third party. Utilizing either approach, the system ensures user privacy and data security. The distribution function 130 interacts with the user through PTD 130 to ship the product to the appropriate location. A variety of distribution systems are contemplated, for example, electronic distribution through a POS terminal coupled to the network, electronic distribution direct to one or more privacy cards and/or digital wallets, or physical product distribution. In one embodiment for physical product distribution, an "anonymous drop-off point", such as a convenience store or other ubiquitous location is used. In another embodiment, it involves the use of a "package distribution kiosk" that allows the user to retrieve the package from the kiosk in a secure fashion. However, in one embodiment, the user may use PTD 170 to change the shipping address of the product at any time during the distribution cycle.

[0025] A user connects to and performs transactions with a secure transaction system (such as shown in **Figure 1**) through a personal transaction device (PTD) that has a unique identifier (ID). In one embodiment, a privacy card is used. In an alternate embodiment a digital wallet is used. In yet another alternate embodiment, a privacy card in conjunction with a digital wallet are used.

[0026] **Figure 2** is a simplified block diagram of one embodiment of a privacy card 205 for a personal transaction device. As illustrated in **Figure 2**, in one embodiment, the card 205 is configured to be the size of a credit card. The privacy card includes a processor 210, memory 215 and input/output logic 220. The processor 210 is configured to execute instructions to perform the

functionality herein. The instructions may be stored in the memory 215. The memory is also configured to store data, such as transaction data and the like. In one embodiment, the memory 215 stores the transaction ID used to perform transactions in accordance with the teachings of the present invention.

Alternately, the processor may be replaced with specially configured logic to perform the functions described here.

[0027] The input/output logic 220 is configured to enable the privacy card 205 to send and receive information. In one embodiment, the input/output logic 220 is configured to communicate through a wired or contact connection. In another embodiment, the logic 220 is configured to communicate through a wireless or contactless connection. A variety of communication technologies may be used.

[0028] In one embodiment, a display 225 is used to generate bar codes scanable by coupled devices and used to perform processes as described herein. The privacy card 205 may also include a magnetic stripe generator 240 to simulate a magnetic stripe readable by devices such as legacy POS terminals.

[0029] In one embodiment, biometric information, such as fingerprint recognition, is used as a security mechanism that limits access to the card 205 to authorized users. A fingerprint touch pad and associated logic 230 is therefore included in one embodiment to perform these functions. Alternately, security may be achieved using a smart card chip interface 250, which uses known smart card technology to perform the function. A suitable biometric control device that may be used is described in United States Patent Application Serial No. 09/510,811, entitled "Method of Using a Personal Device with Internal Biometric

Control in Conducting Transactions Over a Network,” which is herein incorporated by reference.

[0030] Memory 215 can have transaction history storage area. The transaction history storage area stores transaction records (electronic receipts) that are received from POS terminals. The ways for the data to be input to the card include wireless communications and the smart card chip interface which functions similar to existing smart card interfaces. Both of these approaches presume that the POS terminal is equipped with the corresponding interface and can therefore transmit the data to the card.

[0031] Memory 215 can also have user identity/account information block. The user identity/account information block stores data about the user and accounts that are accessed by the card. The type of data stored includes the meta account information used to identify the account to be used.

[0032] **Figure 3** is a simplified block diagram of one embodiment of a digital wallet 305 for a personal transaction device. As illustrated in **Figure 3**, the digital wallet 305 includes a coupling input 310 for the privacy card 205, processor 315, memory 320, input/output logic 225, display 330 and peripheral port 335. The processor 315 is configured to execute instructions, such as those stored in memory 320, to perform the functionality described herein. Memory 320 may also store data including financial information, eCoupons, shopping lists and the like. The digital wallet may be configured to have additional storage. In one embodiment, the additional storage is in a form of a card that couples to the device through peripheral port 310.

[0033] In one embodiment, the privacy card 205 couples to the digital wallet 305 through port 310; however, the privacy card 205 may also couple to the digital wallet 305 through another form of connection including a wireless connection.

[0034] Input/output logic 325 provides the mechanism for the digital wallet 305 to communicate information. In one embodiment, the input/output logic 325 provides data to a point-of-sale terminal or to the privacy card 205 in a pre-specified format. The data may be output through a wired or wireless connection.

[0035] The digital wallet 305 may also include a display 330 for display of status information to the user. The display 330 may also provide requests for input and may be a touch sensitive display, enabling the user to provide the input through the display.

[0036] The physical manifestation of many of the technologies in the digital wallet 305 will likely be different from those in the privacy card 205, mainly because of the availability of physical real estate in which to package technology. Examples of different physical representations would include the display, fingerprint recognition unit, etc.

[0037] The components of a secure transaction system illustrated in **Figures 1, 2, and 3** are further described in International Application published under the Patent Cooperation Treaty (PCT), International Publication Number WO 01/52212, filed on December 28, 2000, and entitled "Secure Electronic Commerce System," which is assigned to the same assignee as the present application and which is hereby incorporated by reference.

Alternatively, multiple users 410 may be connected to TPCB server 440 using corresponding PTDs 420. In the embodiment of **Figure 4**, the user 410 and TPCB 440 communicate via a network implemented in a wired or wireless environment. The network may be the Internet, which is a worldwide system of interconnected networks that runs the Internet Protocol (IP) to transfer data, or other types of networks, such as a token ring network, a local area network (LAN), or a wide area network (WAN).

[0039] PTD 420 further includes a biometric control module 430, which allows PTD 420 to communicate securely with user 410 using biometric information, such as fingerprint recognition. TPC server 440 further includes an access database 450, for example an access list, containing authentication information related to the user 410, for example user identification information and a level of authentication corresponding to the user 410, as described in further detail below. Alternatively, the access database 450 contains authentication information related to multiple users 410, which would uniquely identify other users 410 that may access the secure data.

[0040] In one embodiment, the system 400 further includes secure entity 460, for example a secure server, connected to TPCB server 440 and to PTD 420.

Alternatively, any number of secure entities 460 may communicate with TPCB

server 440. Secure server 460 contains secure data accessible to the user 410 upon completion of an authentication process described in further detail below. In one embodiment, secure server 460 may be another user, similar to user 410, which may share secure data with the user 410 upon completion of the authentication process.

[0041] In one embodiment, secure server 460 is connected to TPCCH server 440 and to PTD 420 via a network implemented in a wired or wireless environment. The network may be the Internet, which is a worldwide system of interconnected networks that runs the Internet Protocol (IP) to transfer data, or other types of networks, such as a token ring network, a local area network (LAN), or a wide area network (WAN). Alternatively, secure server 460 may be connected directly to the PTD 420 via a wired or wireless connection.

[0042] Prior to gaining access to the secure data stored in secure server 460, the user 410 transmits registration information to TPCCH server 440. In one embodiment, the registration information includes identification information for the user 410, such as personal information, specific locations used to access the secure data, and PTD 420 identification information. Alternatively, the transmitted registration information may include other information necessary to identify the user 410, for example, an unlock key provided by biometric control 430 connected to PTD 420.

[0043] In one embodiment, the user identification information includes predetermined access questions specifically tailored by the user 410 to uniquely identify and authenticate the user 410. Alternatively, TPCCH server 440 may

create the predetermined access questions based on the user identification information. The predetermined access questions refer to personal information related to the user 410, which is available only to the user 410 and to TPC server 440.

[0044] Subsequently, TPC server 440 stores the access questions and one or more levels of authentication for the user 410 in a user profile within access database 450. In one embodiment, the level of authentication granted to the user 410 is based on the stored user profile and on the location used to access the secure data. For example, if user 410 is at his or her residence or in the office, full access to the secure data may be granted. However, if user 410 decides to access data from a public kiosk or from a telephone booth, the access may be limited.

[0045] When the user 410 decides to access the secure data stored in secure server 460, PTD 420 associated with the user 410 contacts secure server 460 and transmits an access request to retrieve secure data. Secure server 460 receives the access request and transmits an authentication request to authenticate the user 410. In one embodiment, the authentication request contains a request to provide authentication information related to the user 410, which is requesting access to the secure data.

[0046] In one embodiment, secure server 460 transmits the authentication request directly to TPC server 440. Alternatively, secure server 460 may transmit the authentication request directly to PTD 420. If the authentication

request is transmitted directly to TPD 420, TPD 420 subsequently forwards the authentication request to TPDH server 440.

[0047] After receiving the authentication request, either directly from secure server 460 or through TPD 420, TPDH server 440 retrieves the user profile and the predetermined access questions related to the user 410, and transmits the access questions to PTD 420.

[0048] In one embodiment, the user 410 receives the access questions through PTD 420 and provides answers to the access questions. PTD 420 transmits the answers to the access questions to TPDH server 440. TPDH server 440 receives the answers, authenticates the user 410 to access the secure data, and provides an appropriate level of authentication for the user 410.

[0049] In one embodiment, TPDH server 440 transmits the authentication information directly to secure server 460. Alternatively, TPDH server 440 may transmit the authentication information directly to TPD 420. If the authentication information is transmitted directly to TPD 420, TPD 420 subsequently forwards the authentication information to secure server 460. Finally, secure server 460 grants access to the secure data based on the appropriate level of authentication.

[0050] **Figure 5** is a flow diagram of one embodiment of a method to access secure information related to a user from the perspective of a personal transaction device. As illustrated in **Figure 5**, at processing block 510, PTD 420 transmits registration information to the TPDH server 440. In one embodiment, the registration information includes user identification information and PTD

420 identification information. The user identification information further includes predetermined access questions tailored by the user 410 to uniquely identify the user 410. Alternatively, TPC server 440 creates the predetermined access questions based on the user identification information.

[0051] At processing block 520, PTD 420 contacts secure server 460 and requests access to the secure data. In one embodiment, the user 410 contacts secure server 460 through PTD 420 and transmits an access request to retrieve secure data.

[0052] At processing block 530, a decision is made whether an authentication request is sent directly to TPC server 440. In one embodiment, the secure server 460 transmits the authentication request directly to TPC server 440. Alternatively, the authentication request may be sent to PTD 420.

[0053] If the authentication request is transmitted directly to TPC server 440, then, the process jumps to processing block 555. Otherwise, if the authentication request is not sent through TPC server 440, at processing block 540, PTD 420 receives the authentication request directly from secure server 460. At processing block 550, PTD 420 transmits the authentication request to TPC server 440.

[0054] At processing block 555, TPD 420 receives the predetermined access questions from TPC server 440. At processing block 537, the user 410 provides answers to the access questions and TPD 420 transmits the answers to TPC server 440.

[10055] At processing block 560, another decision is made whether the authentication information is sent directly to secure server 460. In one embodiment, TPC server 440 transmits the authentication information directly to secure server 460. Alternatively, TPC server 440 may transmit the authentication information directly to PTD 420. If the authentication information is transmitted directly to secure server 460, then, at processing block 590, PTD 420 receives access to secure server 460. Otherwise, if the authentication information is not sent directly to secure server 460, at processing block 470, PTD 420 receives the authentication information from TPC server 440.

[0056] At processing block 580, PTD 420 transmits the authentication information to secure server 460. Finally, the process ends at processing block 590, where PTD 420 receives access to secure server 460.

[0057] **Figure 6** is a flow diagram of the method to access secure information related to a user from the perspective of an authentication entity. As illustrated in **Figure 6**, at processing block 610, the authentication entity, for example TPC server 440, receives the registration information from PTD 420.

[0058] At processing block 612, a decision is made whether predetermined access questions were received from PTD 420. If the access questions were not received, at processing block 615, TPC server 440 creates the predetermined access questions based on the user identification information included in the registration information related to the user 410.

[0059] If the access questions were received from PTD 420, at processing block 620, TPCCH server 440 stores authentication information related to the user 410, for example, access questions and one or more levels of authentication, in a user profile within access database 450.

[0060] At processing block 630, a decision is made whether an authentication request is sent directly to TPCCH server 440. In one embodiment, secure server 460 transmits the authentication request directly to TPCCH server 440.

Alternatively, the authentication request may be sent directly to PTD 420.

[0061] If the authentication request is transmitted to TPCCH server 440, then, at processing block 640, the authentication request is received from the secure server 460. Otherwise, if the authentication request is not sent to TPCCH server 440, at processing block 650, the authentication request is received from PTD 420. Subsequently, at processing block 660, authentication information related to the user 410, for example, the user profile containing the predetermined access questions, is retrieved from the access database 450.

[0062] At processing block 665, TPCCH server 440 transmits the access questions to PTD 420. At processing block 667, TPCCH server 440 receives answers to the access questions from PTD 420. In one embodiment, TPCCH server 440 authenticates the user 410 to access the secure data and provides an appropriate level of authentication for the user 410.

[0063] At processing block 670, another decision is made whether the authentication information is sent directly to secure server 460. In one embodiment, at processing block 680, TPCCH server 440 transmits the

authentication information directly to secure server 460. Otherwise, at processing block 690, TPCCH server 440 transmits the authentication information directly to PTD 420.

[0064] **Figure 7** is a flow diagram of the method to access secure information related to a user from the perspective of a secure entity storing the information. As illustrated in **Figure 7**, at processing block 710, secure server 460 receives an access request from PTD 420 connected to the user 410.

[0065] At processing block 720, a decision is made whether an authentication request is sent directly to TPCCH server 440. In one embodiment, at processing block 740, secure server 460 transmits the authentication request directly to TPCCH server 440. Alternatively, at processing block 730, secure server 460 may transmit the authentication request directly to PTD 420.

[0066] At processing block 750, another decision is made whether the authentication information is sent directly to secure server 460. In one embodiment, if the authentication information is sent directly to secure server 460, at processing block 770, secure server 460 receives the authentication information from TPCCH server 440. Alternatively, at processing block 760, secure server 460 receives the authentication information from PTD 420.

[0067] Finally, at processing block 780, based on the authentication information, the secure server 460 transmits the access approval to PTD 420.

[0068] In one embodiment, secure server 460 may be another user, similar to the user 410, and may contain data to be shared among users. In this embodiment, secure server 460 transmits a list of authenticated users to TPCCH server 440,

which uniquely identifies other users 410 that may access the information, as described in detail above. TPCCH server 440 may then store authentication information related to each authenticated user 410 of the multiple authenticated users present on the list and may determine access rights for any user 410 trying to retrieve shared data from secure server 460.

[0069] **Figure 8** is a block diagram of an exemplary digital processing or computing system 800 in which the present invention can be implemented. For example, digital processing system 800 can represent TPCCH server 440 or personal transaction device 420, as described in **Figure 4**. Digital processing system 800 may store a set of instructions for causing the system to perform any of the operations described above. Digital processing system 800 can also represent a network device, which includes a network router, switch, bridge, or gateway.

[0070] Referring to **Figure 8**, digital processing system 800 includes a bus 808 coupled to a central processing unit (CPU) 802, main memory 804, static memory 806, network interface 822, video display 810, alpha-numeric input device 812, cursor control device 814, drive unit 816, and signal generation device 820. The devices coupled to bus 808 can use bus 808 to communicate information or data to each other. Furthermore, the devices of digital processing system 800 are exemplary in which one or more devices can be omitted or added. For example, one or more memory devices can be used for digital processing system 800.

[0071] The CPU 802 can process instructions 826 stored either in main memory 804 or in a machine-readable medium 824 within drive unit 816 via bus 808. For

[0072] Main memory 804 can be, e.g., a random access memory (RAM) or some other dynamic storage device. Main memory 804 stores instructions 826, which can be used by CPU 802. Main memory 804 may also store temporary variables or other intermediate information during execution of instructions by CPU 802. Static memory 806 can be, e.g., a read only memory (ROM) and/or other static storage devices, for storing information or instructions, which can also be used by CPU 802. Drive unit 816 can be, e.g., a hard or floppy disk drive unit or optical disk drive unit, having a machine-readable medium 824 storing instructions 826. The machine-readable medium 824 can also store other types of information or data.

[0073] Video display 810 can be, e.g., a cathode ray tube (CRT) or liquid crystal display (LCD). Video display device 810 displays information or graphics to a user. Alphanumeric input device 812 is an input device (e.g., a keyboard) for communicating information and command selections to digital processing system 800. Cursor control device 814 can be, e.g., a mouse, a trackball, or cursor direction keys, for controlling movement of an object on video display 810. Signal generation device 820 can be, e.g., a speaker or a microphone.

[0074] Digital processing system 800 can be connected to a network 801 via a network interface device 822. Network interface 822 can connect to a network

such as, for example, a local area network (LAN), wide area network (WAN), token ring network, Internet, or other like networks. Network interface device 822 can also support varying network protocols such as, for example, hypertext transfer protocol (HTTP), asynchronous transfer mode (ATM), fiber distributed data interface (FDDI), frame relay, or other like protocols.

[0075] It is to be understood that embodiments of this invention may be used as or to support software programs executed upon some form of processing core (such as the CPU of a computer) or otherwise implemented or realized upon or within a machine or computer readable medium. A machine readable medium includes any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer). For example, a machine readable medium includes read-only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.); or any other type of media suitable for storing or transmitting information.

[0076] The invention has been described in conjunction with the preferred embodiment. It is evident that numerous alternatives, modifications, variations and uses will be apparent to those skilled in the art in light of the foregoing description.